REMARKS

This amendment is in response to the office action dated January 11, 2006. Claims 1-38 were pending in the application as of this office action, including independent claims 1, 26, 32 and 34-36.

Claims 1, 3, 8-11, 13-16, 23, 34 and 37 stand rejected under 35 U.S.C. 102(e) as being allegedly anticipated by U.S. Pat. No. 6,772,340 ("Peinado").

Claim 2 stands rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Peinado in view of U.S. Pat. No. 6,336,189 ("Takeda").

Claims 4-7, 17, 32, 33 and 36 are rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Peinado in view of U.S. Pat. No. 6,069,957 ("Richards").

Claims 12, 24, 26-29 and 35 are rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Peinado and further in view of Stallings, *Cryptography and Network Security* ("Stallings").

Claims 18-22, 30, 31 and 38 are objected to as depending from rejected base claims, but are otherwise allowable. Claims 25 and 37 are objected to for the same reason, and under the second paragraph of 35 U.S.C. 112.

Claims 3 and 37 are canceled. Claims 1, 6, 8, 10, 11, 13, 25, 26, and 34 are amended.

I. Claims rejected under 35 U.S.C. § 112

A. Claims 25 and 37

The examiner asserts that claim 25 is "incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections." The examiner objects to the phrase "wherein the rights management file enables access to the private key." The examiner stated that claim 25 would be allowable if this objection were overcome.

Claim 25 has been amended. Because claim 25 depends from claim 24 which the applicant believes is in condition for allowance, see below, the applicant submits that claim 25 is now also in condition for allowance.

The examiner asserted, "Claim 37 recites the limitation 'the set of permission rights' in line 1. There is insufficient antecedent basis for this limitation in the claim."

The rejection of claim 37 is moot in light of its cancellation. The cancellation is made without prejudice.

II. Claims rejected under 35 U.S.C. § 102

A. Claims 1, 3, 8-11, 13-16, 23, 34 and 37

The rejection of claims 3 and 37 is moot in light of their cancellation. The limitations of claim 3 have been incorporated into claim 1.

Claim 1 recites a computer-implemented method for managing access to electronic documents. The claim recites associating a first key with an encrypted document decryption key. The encrypted document decryption key is associated with an encrypted document. The encrypted document decryption key, when decrypted, yields a document decryption key usable to decrypt the encrypted document. The first key is usable to decrypt the encrypted document decryption key. The first key is itself encrypted, associated with a second key that can be used to decrypt the encrypted first key. This second key is provided in an access controlled manner to users for use in opening all documents that can be opened through use of the first key.

Peinado discloses encrypted content which can be decrypted by a decryption key KD. KD is itself encrypted, so to use the encrypted KD key, the encrypted KD key must first be decrypted by the black box with its private key, PR-BB. The black box controls access to the PR-BB key depending on whether the user complies with a "license," which may depend on the user's identity, state information such as how many times the content has been read, a machine-specific identifier, etc. See column 23 line 58 to column 24, line 10, as well as column 18, lines 9-25.

The examiner stated that Peinado discloses an encrypted document key, an encrypted first key, and a second key. The applicant disagrees. Even if one assumes for argument's sake that KD corresponds to the encrypted document key and PR-BB corresponds to the first key, Peinado does not disclose the second key.

The examiner looks to column 23, lines 6-24 of Peinado for the limitation of having a second key. There Peinado discloses a way of hiding a private key from the world. (A "private key" is part of a private-key and public-key pair for use in public-key cryptography.) Peinado teaches that one way to hide this private key is to split it into several sub-components, encrypting each sub-component separately, then storing each separately in a different location. That is to say, Peinado teaches splitting *one* private key into several pieces. No piece is useful on its own, because each is only a piece of a key and not a whole key. By teaching only a single private key, Peinado does not teach two separate keys (a first key and a second key). In particular Peinado does not teach a second key which encrypts a first key, where the first key encrypts a document decryption key.

Additionally, even if assuming for argument's sake that the PR-BB key corresponds to the recited first key, Peinado does not teach that the PR-BB key is encrypted.

For at least these reasons, the applicant submits that claim 1, as well as claims 8-11, 13-16, and 23, which depend from claim 1, are in condition for allowance. Claim 34 incorporate a similar limitation and are in condition for allowance for at least the same reason.

Claim 10 depends from claim 1 and additionally recites that providing the second key in an access controlled manner to users includes sending information used to synthesize the second key. The information is sent in rights management information.

Peinado discloses generating a digital license for digital content by a license server after negotiation with an user. The license includes the content ID of the digital content, the rights description, the decryption key for the digital content (the key itself possibly being encrypted), a digital signature encrypted with the license server's private key, and a certificate from the content server. The license is transmitted to the user's computer, which then stores the license. Peinado does not disclose sending information to users to synthesize the first key. See column 21, lines 11-62.

In Peinado the only information sent to the user is the digital license. Peinado teaches that the digital license does not include information for the user to synthesize a key; instead, the decryption key is itself actually sent to the user. By contrast claim 10 recites "sending information used to synthesize the second key."

For at least this reason, the applicant respectfully submits that claim 10 as well as claim 16, which depends from claim 10, are in condition for allowance.

Claim 13 depends from claim 1 and further recites providing the document decryption key in an access controlled manner to users for use in opening the encrypted document without using the first key.

Peinado discloses a black box and a license evaluator. The black box decrypts a decryption key used to decrypt encrypted digital content. The black box works with the license evaluator to ascertain whether an user is privileged to access the digital content. After it has been so ascertained, the black box is provided with a decryption key for the encrypted digital content. The black box must perform decryption only in accordance with the license and must not continue to operate if tampered with, see column 15, line 53 to column 16, line 4 which reads in full:

> DRM System 32 Components--Black Box 30
>
> Primarily, and as was discussed above, the black box 30 performs encryption and decryption functions in the DRM system 32. In particular, the black box 30 works in conjunction with the license evaluator 36 to decrypt and encrypt certain information as part of the license evaluation function. In addition, once the license evaluator 36 determines that a user does in fact have the right to render the requested digital content 12 in the manner sought, the black box 30 is provided with a decryption key (KD) for such digital content 12, and performs the function of decrypting such digital content 12 based on such decryption key (KD).
>
> The black box 30 is also a trusted component in the DRM system 32. In particular, the license server 24 must trust that the black box 30 will perform the decryption function only in accordance with the license rules in the license 16, and also trust that such black box 30 will not operate should it become adulterated or otherwise modified by a user for the nefarious purpose of bypassing actual evaluation of a license 16.

The encrypted decryption key is obtained from the license, and by implication nowhere else, see column 23, lines 64-67. "Specifically, to render the requested digital content 12, the license evaluator 36 and the black box 30 in combination obtain the decryption key (KD) from such license 16, and the black box 30 employs such decryption key (KD) to decrypt the digital content 12."

The decryption key is encrypted with the black box public key, which means it is decoded with the black box's private key, see column 24, lines 59-61. "the decryption key (KD) for the digital content 12 encrypted with the black box 30 public key (PU-BB) (i.e., (PU-BB (KD));"

The examiner stated that Peinado teaches "providing a document decryption key in an access-controlled manner to users for accessing the document without using the first key," looking to column 15, line 53 to column 16, line 4. The applicant disagrees, because that same cited text supports the opposite conclusion, see above.

Peinado teaches that there is precisely one way to decrypt digital content: by using the black box's private key to decrypt the license's encrypted decryption key, and then using that decryption key to decrypt the digital content. Even assuming for argument's sake that Peinado's decryption key corresponds to the applicant's document encryption key and Peinado's black box private key corresponds to the applicant's first key, Peinado does not teach any way of providing the document decryption key without using the first key. By contrast, claim 13 recites "providing a document decryption key in an access-controlled manner to users for accessing the document without using the first key."

For at least this reason, the applicant submits that claim 13 is in condition for allowance.

III. Claims rejections under 35 U.S.C. § 103

A. Claims 4-7, 17, 32, 33 and 36

Claims 4-7 and 17 depend from claim 1. The cited portions of Richards do not overcome the deficiencies of Peinado with respect to claim 1. Therefore, claims 4-7 and 17 are also in condition for allowance for at least the same reasons as claim 1.

Claim 32 recites a method for managing access to encrypted electronic documents. The method provides in an access controlled manner multiple skeleton decryption keys for multiple encrypted documents. A single skeleton key can be used to open multiple encrypted documents and a single encrypted document can be opened using more than one skeleton key. A single skeleton key can be opened using one or more other skeleton keys. Each single skeleton key is a key usable to decrypt one or more secondary decryption keys, which itself is either a skeleton key or a decryption key for an encrypted document. One or more skeleton keys can be issued for a document or a set of documents, and a holder of a particular skeleton key can open any document to which the particular skeleton key applies, directly or indirectly.

Richards discloses restricting access to television programs using a key hierarchy, or "key-upon-key" encryption, as explained above in the remarks for claims 4 and 17.

The examiner says that Richards discloses the features of "a single skeleton key [that] can be used to open multiple encrypted documents [and] a single encrypted document [that] can be opened using more than one skeleton key." The applicant disagrees.

The examiner seems to believe that SK keys are equivalent to skeleton keys, because the cited to sections exclusively discuss SK keys, see column 7, lines 24-33, and column 8, lines 44-64. The SK keys of Richards are not skeleton keys, because they do not open more than one television program. Richards discloses that television programs CONTENT_A, CONTENT_B, etc. are encrypted with keys SK_A, SK_B, etc., see column 8, lines 37-44. In other words "each program is encrypted using a different key," see column 8, lines 36-37. By contrast the SK keys decrypt digital content, in particular television programs.

The PK key of Richards is not a skeleton key, either. The SK keys are encrypted with a single PK key. Although the PK changes over time, Richards does not disclose any SK key being encrypted with two or more different PK keys, see column 10, lines 13-18. Therefore, the data protected by any individual SK key cannot be opened indirectly by two or more different PK keys. The applicant, by contrast, claims "a single encrypted document can be opened using more than one skeleton key." Therefore, a PK key is not equivalent to a skeleton key.

The CUSTOMER_CODE of Richards is not equivalent to a skeleton key, either. The CUSTOMER_CODE keys are used to encrypt PK keys, however the CUSTOMER_CODE keys are never themselves encrypted, only "extremely well concealed," let alone encrypted with another CUSTOMER_CODE key, see column 10, lines 56-64. The applicant, by contrast, claims "a single skeleton key can be opened using one or more other skeleton keys." Therefore, a CUSTOMER_CODE is not equivalent to a skeleton key. Richards does not disclose skeleton keys as defined by the applicant.

The relied upon portions of Peinado do not remedy the deficiencies.

For at least these reasons, the applicant submits that claim 32 as well as claim 33, which depends from claim 32, are in condition for allowance. Claim 36 incorporates a similar limitation and is in condition for allowance for at least the same reason.

B. Claims 12, 24, 26-29 and 35

Claims 12 and 24 depend from claim 1. The cited portions of Stallings do not overcome the deficiencies of Peinado with respect to claim 1. Therefore, claims 12 and 24 are also in condition for allowance for at least the same reasons as claim 1.

Claim 26 recites obtaining an encrypted electronic document and obtaining a collection of at least three keys, the keys including keys that are encrypted. The keys and the document have associations defined between certain pairs of them. Each association of a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key. Each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document. The claim further recites that a user has access to and can use certain ones of the keys in the collection. The claim also recites using the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, to which the user has access.

The cited portion of Stallings describes sending an identifier Key ID for a public key KU_b in a message containing encrypted data so that a receiver of a message (usually) knows what private key to use to decrypt a session key K_s. The session key can then be used to decrypt the message data, see Stallings, pp. 363-364 and Fig. 12.3. That is to say, Stallings uses a Key ID to identify (with high probability) the *single* private key which can successfully decrypt the session key.

The examiner says that Peinado does not explicitly disclose "defining the associations." He looks to Stallings, "wherein one of the salient features ... defines an association between an encrypted data encryption key and a key-decrypting key, and between the encrypted data-decrypting key and the encrypted document, to efficiently identify which keys are sufficient to decrypt the encrypted document."

Assuming for the sake of argument that the Key ID in Stallings associates a pair consisting of a private key with an encrypted session key, Stallings does not disclose a collection of at least three keys, as recited.

For at least this reason, the applicant respectfully submits that claim 26 as well as claims 27-29, which depend from claim 26, are in condition for allowance. Claim 35 incorporates a similar limitation and is in condition for allowance for at least the same reason.

Please charge Deposit Account No. 06-1050 for the Petition for Extension of Time fee. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 5/11/06

Daniel J. Burns
Reg. No. 50,222

Customer No. 021876
Fish & Richardson P.C.
500 Arguello Street, Suite 500
Redwood City, California 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

50326285.doc